AF/IFW
$

GUNNISON, McKAY & HODGSON, L.L.P.
GARDEN WEST OFFICE PLAZA, SUITE 220
1900 GARDEN ROAD
MONTEREY, CALIFORNIA 93940
(831) 655-0880
FACSIMILE (831) 655-0888

November 30, 2007

Mail Stop Appeal Brief--Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL LETTER

RE:	Applicant(s):	Peter Szor		
	Assignee:	Symantec Corporation		
	Title:	SIGNATURE EXTRACTION SYSTEM AND METHOD		
	Serial No.:	10/611,472	Filed:	June 30, 2003
	Examiner:	Ronald Baum	Group Art Unit:	2136
	Docket No.:	SYMC1034		

Dear Sir:

Transmitted herewith are the following documents in support of the Notice of Appeal filed on October 17, 2007:

1. Return receipt postcard;
2. Check in the amount of $510.00 for filing a brief in support of an appeal;
3. This Transmittal Letter (2 pages); and
4. Appellant's Brief (27 pages).

☒ Conditional Petition for Extension of Time: If an extension of time is required for timely filing of the enclosed documents after all papers filed with this transmittal have been considered, Applicants hereby petition for such an extension of time.

☒ The Commissioner is hereby authorized to charge any additional fees required for consideration of the enclosed documents, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on November 30, 2007.

Attorney for Applicant(s)

November 30, 2007
Date of Signature

Respectfully submitted,

Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s):	Peter Szor		
Assignee:	Symantec Corporation		
Title:	SIGNATURE EXTRACTION SYSTEM AND METHOD		
Serial No.:	10/611,472	Filed:	June 30, 2003
Examiner:	Ronald Baum	Group Art Unit:	2136
Docket No.:	SYMC1034		

Monterey, CA
November 30, 2007

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF

Dear Sir:

Pursuant to 37 CFR § 41.37(a)(1), Appellant files this Appellant's Brief in support of the Notice of Appeal filed on October 17, 2007.

Real Party in Interest

The assignee of the above-referenced patent application, Symantec Corporation, is the real party in interest.

RELATED APPEALS AND INTERFERENCES

No other prior and pending appeals, judicial proceedings or interferences are known to appellant, the appellant's legal representative, or Assignee, which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

Status of Claims

Claims 1-16, 19-33 are pending in the application.

Claims 1-16, 19-32 are rejected. The rejection of Claims 1-16, 19-32 is hereby appealed.

Claim 33 stands objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claims and any intervening claims.

Status of Amendments

All amendments have been entered.

Summary of Claimed Subject Matter

Regarding independent Claims 1, 27, referring to FIGS. 1 and 3 together, Applicant's specification sets forth:

> In **attack check operation 204**, a determination is made as to whether a suspected or actual attack, a malicious exploit, use of common exploit tools such as an autorooter, **hereinafter referred to as an attack** for simplicity of discussion, **has occurred on host computer system 104A**. (page 7, lines 5-9, emphasis added.)
>
> In **extract malicious code signature operation 304, the signature, sometimes called malicious code signature, of the malicious code is extracted.** For example, a custom size signature from the malicious code is extracted using an extraction engine. In one embodiment, **the malicious code signature is 32 bytes of the malicious code extracted backwards from the callers address. A signature is a specific sequence of information, e.g., bytes**. (Page 16, lines 9-16, emphasis added.)
>
> More particularly, **in create extracted malicious code packet operation 214A, an extracted malicious code packet is created.** In one embodiment, **an extracted malicious code packet is a collection of information which includes** the malicious code parameters appended in append malicious code parameters operation 212A and **the extracted malicious code signature extracted in extract malicious code signature operation 304**. (Page 17, lines 27-34, emphasis added.)
>
> In **send packet operation 222, the extracted malicious code packet created in create extracted malicious code packet operation 214 is sent from host computer system 104A**. … In one embodiment, **the extracted malicious code packet is sent to local analysis center computer system 112** as discussed further below in reference to FIG. 4. In another embodiment, the extracted malicious code packet is sent directly to global analysis center 116. In yet another embodiment, the extracted malicious code packet is sent to both local analysis center computer system 112 and global analysis center 116. (Page 14, line 37 to page 15, line 19, emphasis added.)

Regarding independent Claims 5, 28, referring to FIGS. 1 and 2 together, Applicant's specification sets forth:

> In **attack check operation 204**, a determination is made as to whether a suspected or actual attack, a malicious exploit, use of common exploit tools such as an autorooter, **hereinafter referred to as an attack** for simplicity of discussion, **has occurred on host computer system 104A**. (page 7, lines 5-9, emphasis added.)
>
> For example, in one embodiment, **parameters associated with the malicious code include the caller's address such as the location of the sendto() API of the malicious code, the name of the process in which the attack took place, the ports connected to this process, the send() API's connected ports such as UDP 1434, the service pack levels, the operating system information, and patch level information.**
> From append malicious code parameters operation 212, flow moves to a create extracted malicious code packet operation 214. **In create extracted malicious code packet operation 214, an extracted malicious code packet is created.** In one embodiment, **an extracted malicious code packet is a collection of information which includes the malicious code parameters appended in append malicious code parameters operation 212 and either the extracted malicious code or the extracted malicious code snippet depending upon whether extract malicious code operation 208 or extract malicious code snippet operation 210, respectively, is performed.** (Page 10, lines 14-31, emphasis added.)
>
> In **send packet operation 222, the extracted malicious code packet created in create extracted malicious code packet operation 214 is sent from host computer system 104A.** … In one embodiment, **the extracted malicious code packet is sent to local analysis center computer system 112** as discussed further below in reference to FIG. 4. In another embodiment, the extracted malicious code packet is sent directly to global analysis center 116. In yet another embodiment, the extracted malicious code packet is sent to both local analysis center computer system 112 and global analysis center 116. (Page 14, line 37 to page 15, line 19, emphasis added.)

Regarding independent Claims 16, 29, referring to FIGS. 1 and 4 together, Applicant's specification sets forth:

> In **receive packet check operation 404**, a determination is made as to whether an extracted malicious code packet has been received by local analysis center computer system 112. As discussed above, **an extracted malicious code packet is sent from host computer system 104A** in send packet operation 222 of FIGS. 2 and 3 to **local analysis center computer center 112**. (Page 21, lines 22-28, emphasis added.)
>
> In **attack threshold exceeded check operation 408**, a determination is made as to whether **an attack threshold has been exceeded.** An attack threshold is a minimum threshold of suspicious activity associated with the received extracted malicious code packets to results in a conclusion that an attack has occurred on client network 120. (Page 22, lines 19-24, emphasis added.)
>
> In create signature update operation 412, a **signature update for intrusion detection system 108 is created.** For example, a definition file for use by intrusion detection system 108 **is updated with the malicious code signature** extracted during extract malicious code signature operation 406 or received with the extracted malicious code packet during check operation 404. (Page 23, lines 23-29, emphasis added.)
>
> In **deliver signature update operation 416**, the **signature update** created in create signature update operation 412 is sent from local analysis center computer system 112. In one embodiment, **the signature update is sent to intrusion detection system 108.** In another embodiment, the signature update is sent directly to global analysis center 116. In yet another embodiment, **the signature update is sent to both intrusion detection system 108** and global analysis center 116. (Page 24, lines 24-32, emphasis added.)

Regarding dependent Claim 13, referring to FIGS. 1 and 2 together, Applicant's specification sets forth:

> In **extract malicious code snippet operation 210, a snippet, sometimes called portion, of the malicious code is extracted** from the memory location. As

> discussed above, in one embodiment, behavior blocking application 126A provides the memory location, sometimes called the caller’s address, of the malicious code. Accordingly, in one embodiment, **a snippet (portion) of the malicious code is copied or cut, sometimes called removed, from the memory location during extract malicious code snippet operation 210**. For example, a portion of the content of a buffer containing the malicious code is copied or cut.
>
> To illustrate, in one embodiment, the caller’s address is the memory location of the instruction or set of instructions that originated the critical operating system function call. **A portion of the malicious code around, e.g. at addresses above and below, the caller's address is extracted in extract malicious code snippet operation 210**. In one particular embodiment,+-4KB of code around the caller's address is extracted although more or less than +-4KB of code are extracted other embodiments. (Page 9, line 21 to page 10, line 3, emphasis added.)

Grounds of rejection to be reviewed on appeal

1. Whether Claims 1-16, 19-32 are unpatentable under 35 U.S.C. 103(a) over Magdych et al. (6,546,493) in view of Hollander et al. (6,412,071)?

Argument

1. Claims 1-16, 19-32 are patentable over Magdych et al. (6,546,493) in view of Hollander et al. (6,412,071).

The Examiner states:

> As per claim 1; "A method comprising: … extracting a malicious code signature from said malicious code [*Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 3,lines 23-49, whereas the comparison of 'a plurality of virus/attack signatures …* ***or extract the harmful information from the infected communications*** *…' aspects of the intrusion/attack detection/risk assessment/remediation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.*] comprising: locating a caller's address of said malicious code in a memory of said first computer system; and extracting a specific number of bytes backwards from said caller's address; creating an extracted malicious code packet including said malicious code signature [*Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., separate intrusion/attack detection (first computer) system versus the risk assessment/remediation (second computer) system* ***where the first to second extracted malicious code information clearly is transferred in a coded packet****), clearly encompasses the claimed limitations as broadly interpreted by the examiner.*]; …(Final Office Action dated August 20, 2007, pages 2-3, emphasis added.)

The Examiner's statement is respectfully traversed. As set forth in the Amendment filed on May 31, 2007 at page 11:

As set forth further below, Magdych et al. teaches: 1) network communications **between** networked devices are scanned; and 2) harmful information from an infected communication is **extracted to disinfect the communication.**

More particularly, Magdych et al. teaches:

> … The intrusion detection tool 112 detects attacks or intrusions by **scanning network communications between the various foregoing network devices**. Of course, the intrusion detection tool 112 may also be capable of scanning executable files, application macro files, disk boot sectors, etc. This scanning may include comparing the network communications, etc. with a plurality of virus/attack signatures, known vulnerabilities and/or policies that may be constantly updated. Upon the detection of any of these by the intrusion detection tool 112, a remedying event may then be used to execute a risk assessment scan, report the problem, quarantine the infected communications, and/or **extract the harmful information from the infected communications**, thereby **disinfecting the communications**. (Col. 3, lines 35-48, emphasis added.)

Accordingly, the Examiner has failed to callout where Magdych et al. teaches or suggests "locating a caller's address of said malicious code in a memory of said first computer system; and extracting a specific number of bytes backwards from said caller's address" as asserted by the Examiner. In fact, the Examiner admits:

> The teachings of Magdych et al suggest the base claims limitations … ***without explicitly teaching*** of the use of "…**locating a caller's address of said malicious code in a memory of said first computer system; and extracting a specific number of bytes backward from said caller's address**", as a form of specific malicious code address extraction for the purpose of signature construction functionality per se. (Final Office Action dated August 20, 2007, page 23, emphasis added.)

Hollander et al. does not cure this glaring deficiency in Magdych et al. Regarding Hollander et al., the Examiner states:

> Hollander et al, teaches (i.e., Abstract, figures 1-8 and associated descriptions, col. 2, lines 23-67, col. 3, lines 40-col. 4, line 8) of detecting, preventing/notification generation thereof, of buffer overflow events in real time such that the API Interception System model is used as a basis to tag

> calls to executing code and determine specific characteristics of the calling/called code (i.e., either as it is referenced in memory or more particularly as it's address as contained in a location in the stack that should have contained the real return address prior to the buffer overflow attack.) The **Hollander et al invention also clearly encompasses the collection of the stack/frame involved in the area of memory associated with the address of malicious code** (i.e., '*extracting a specific number of bytes backward from said caller's address*'), insofar as the preventing/notification aspects associated with the applicants claimed invention. (Final Office Action dated August 20, 2007, page 24, emphasis added.)

The Examiner's statement is respectfully traversed. Hollander et al. teaches that a call or caller routine address validity is examined by comparing the call originating address or caller routing address with a range of addresses. To illustrate, Hollander et al. teaches:

> … The method of secure function execution comprises the steps of examining the intercepted system call validity by comparing the **intercepted system call originating address** with **range of process valid addresses** associated with the process from which the intercepted system call originated. … A method of secure function execution examines the intercepted library call validity by comparing **the intercepted library call originating address** with **range of process valid addresses** associated with the process from which the intercepted library call originated. … The method comprises the steps of receiving a caller routine return address from the process memory device and determining whether the caller routine address is valid by comparing **the caller routine address with a process valid address table**. … The method comprises the steps of receiving a caller routine return address from said process memory device and determining whether the caller routine address is valid by comparing the **caller routine address with an associated process stack address area**. (Col. 2, lines 24-67, emphasis added.)

Further, if the call is illegal, Hollander et al. teaches that the illegal function is terminated, the user is notified about the illegal call, or a user predetermined action is performed. To illustrate, Hollander et al. teaches:

> SFE Server 116 determines whether said system call is valid by comparing said system call originating memory address with the range of Process Valid Address Range List associated with said process from which said system call originated. **If an illegal call was detected** the SFE Server 116 may **terminate the illegal function** (step 164). Alternatively SFE Server 116 **may notify a user (typically the System Administrator) about the illegal call** (step 166). Alternatively, SFE Server 116 may **perform another or other series of user predetermined actions** (step 166). (Col. 7, lines 53-62, emphasis added.)

Accordingly, the Examiner has failed to callout where Hollander et al. teaches or suggests "the collection of the stack/frame involved in the area of memory associated with the address of malicious code (i.e., '*extracting a specific number of bytes backward from said caller's address*')" as asserted by the Examiner.

For at least the above reasons, Magdych et al. in view of Hollander et al. does not teach or suggest:

> A method comprising:
> detecting an attack by malicious code on a first computer system;
> extracting a malicious code signature from said malicious code comprising:
> **locating a caller's address of said malicious code in a memory of said first computer system;** and
> **extracting a specific number of bytes backwards from said caller's address;**
> **creating an extracted malicious code packet including said malicious code signature**; and
> sending said extracted malicious code packet from said first computer system to a second computer system,

as recited in Claim 1, emphasis added. For at least the above reasons, Claim 1 is allowable over Magdych et al. in view of Hollander et al.

Claims 2-4, 30, which depend from Claim 1, are allowable for at least the same reasons as Claim 1. Claim 27 is allowable for reasons similar to Claim 1.

For similar reasons, Magdych et al. in view of Hollander et al. does not teach or suggest:

> A method comprising:
> detecting an attack by malicious code on a first computer system;
> **creating an extracted malicious code packet including parameters associated with said malicious code**, said parameters being selected from the group consisting of a caller's address of said malicious code in a memory of said first computer system, a name of a process in which said attack took place, ports connected to said process, service pack levels, operating system information, patch level information, and combinations thereof; and
> sending said extracted malicious code packet from said first computer system to a second computer system,

as recited in Claim 5, emphasis added. Accordingly, Claim 5 is allowable. Claims 6-15, 31-32, which depend from Claim 5, are allowable for at least the same reasons as Claim 5. Claim 28 is allowable for reasons similar to Claim 5.

For similar reasons, Magdych et al. in view of Hollander et al. does not teach or suggest:

> The method of Claim 9 wherein upon a determination that said malicious code is not sendable, said method further comprising **extracting a snippet of said malicious code from a memory location**,

as recited in dependent Claim 13, emphasis added. For at least this additional reason, Claim 13 is allowable. Claims 14-15, 32, which depend from Claim 13, are additionally allowable for at least the same reasons as Claim 13.

Regarding Claim 16, the Examiner states:

> As per claim 16; "A method comprising:… wherein upon a determination that an attack threshold has been

> exceeded, said method further comprising delivering a signature update comprising a malicious code signature to an intrusion detection system [*Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 2,lines 27-55, whereas the comparison of '… **a database on known vulnerabilities may then be updated [i.e., at the 'intrusion detection system'] based on risk assessment scan** …' aspects of the intrusion/attack detection/risk assessment/remediation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.*]". (Final Office Action dated August 20, 2007, pages 14-15, emphasis added.)

In response to the Examiner's statement, as set forth in the Amendment filed on May 31, 2007 at pages 13-14:

Accordingly, Magdych et al. teaches a feedback mechanism between the risk assessment scanning tool 110 and the intrusion detection tool 112. Specifically, Magdych et al. teaches:

> Once complete, the results in the form of any additional known vulnerabilities are outputted in operation 510. As an option, the results may be used to update the database of threats (i.e. vulnerabilities and polices) mentioned hereinabove in operation 302 of FIG. 3. Note operation 512. As such, fixture use of such database by the intrusion detection tool 112 may include the known vulnerabilities outputted in operation 510. Thus, **there is a feedback mechanism between the risk assessment scanning tool 110 and intrusion detection tool 112**. (Col. 7, lines 1-10, emphasis added.)

For at least the above reasons, Magdych et al. does not teach or suggest:

> A method comprising:
>
> receiving an **extracted malicious code packet from a first computer system** with a second computer system, **said first computer system being a host computer system and said second computer system being a local analysis center computer system**; and

> determining whether an attack threshold has been exceeded based upon said extracted malicious code packet, wherein upon a determination that an attack threshold has been exceeded, said method further comprising **delivering a signature update comprising a malicious code signature to an intrusion detection system**,

as recited in Claim 16, emphasis added.

Hollander et al. does not cure this deficiency in Magdych et al. Accordingly, Claim 16 is allowable over Magdych et al. in view of Hollander et al. Claims 19-26, which depend from Claim 16, are allowable for at least the same reasons as Claim 16. Claim 29 is allowable for reasons similar to Claim 16.

For at least the above reasons, Applicant respectfully requests that this rejection be reversed.

Claims appendix

1. (Previously presented) A method comprising:

detecting an attack by malicious code on a first computer system;

extracting a malicious code signature from said malicious code comprising:

locating a caller's address of said malicious code in a memory of said first computer system; and

extracting a specific number of bytes backwards from said caller's address;

creating an extracted malicious code packet including said malicious code signature; and

sending said extracted malicious code packet from said first computer system to a second computer system.

2. (Original) The method of Claim 1 wherein prior to said sending, said method further comprising determining that said extracted malicious code packet is a new extracted malicious code packet.

3. (Original) The method of Claim 1 wherein prior to said sending, said method further comprising determining that a maximum number of extracted malicious code packets have not been sent from said first computer system.

4. (Original) The method of Claim 1 wherein said extracted malicious code packet is sent from said first computer system to said second computer system on a secure channel.

5. (Previously presented) A method comprising:

detecting an attack by malicious code on a first computer system;

creating an extracted malicious code packet including parameters associated with said malicious code, said parameters being selected from the group consisting of a caller's address of said malicious code in a memory of said first computer system, a name of a process in which said attack took place, ports connected to said process, service pack levels, operating system information, patch level information, and combinations thereof; and

sending said extracted malicious code packet from said first computer system to a second computer system.

6. (Original) The method of Claim 5 wherein prior to said sending, said method further comprising determining that said extracted malicious code packet is a new extracted malicious code packet.

7. (Original) The method of Claim 5 wherein prior to said sending, said method further comprising determining that a maximum number of extracted malicious code packets have not been sent from said first computer system.

8. (Original) The method of Claim 5 wherein said extracted malicious code packet is sent from said first computer system to said second computer system on a secure channel.

9. (Original) The method of Claim 5 further comprising determining whether said malicious code is sendable.

10. (Original) The method of Claim 9 wherein upon a determination that said malicious code is sendable, said method further comprising extracting said malicious code from a memory location.

11. (Original) The method of Claim 10 wherein said extracting comprises copying or cutting said malicious code from said memory location.

12. (Original) The method of Claim 10 further comprising appending said parameters to said malicious code after said extraction.

13. (Original) The method of Claim 9 wherein upon a determination that said malicious code is not sendable, said method further comprising extracting a snippet of said malicious code from a memory location.

14. (Original) The method of Claim 13 wherein said extracting comprises copying or cutting a portion of said malicious code from said memory location.

15. (Original) The method of Claim 13 further comprising appending said parameters to said snippet after said extraction.

16. (Previously presented) A method comprising:

receiving an extracted malicious code packet from a first computer system with a second computer system, said first computer system being a host computer system and said second computer system being a local analysis center computer system; and

determining whether an attack threshold has been exceeded based upon said extracted malicious code packet, wherein upon a determination that an attack threshold has been exceeded, said method further comprising delivering a signature update comprising a malicious code signature to an intrusion detection system.

17-18. (Canceled)

19. (Previously presented) The method of Claim 16 further comprising determining that a maximum number of signature updates have not been sent prior to said delivering a signature update.

20. (Previously presented) The method of Claim 16 further comprising creating said signature update.

21. (Original) The method of Claim 16 wherein said extracted malicious code packet includes a malicious code signature, and wherein upon a determination that said attack threshold has been exceeded, said method further comprising delivering said malicious code signature to a global analysis center.

22. (Original) The method of Claim 21 further comprising determining that a maximum number of malicious code signatures have not been sent prior to said delivering said malicious code signature.

23. (Original) The method of Claim 21 further comprising extracting said malicious code signature from said extracted malicious code packet.

24. (Original) The method of Claim 16 further comprising determining whether said extracted malicious code packet includes a malicious code signature, wherein upon a determination that said extracted malicious code packet does not include a malicious code signature, said method further comprising extracting a malicious code signature from said extracted malicious code packet.

25. (Original) The method of Claim 16 wherein upon a determination that said attack threshold has been exceeded, said method further comprising delivering said extracted malicious code packet to a global analysis center.

26. (Original) The method of Claim 25 further comprising determining that a maximum number of extracted malicious code packets have not been sent prior to said delivering said extracted malicious code packet.

27. (Previously presented) A computer system comprising:

an intrusion prevention application for detecting an attack by malicious code on a first computer system;

a host signature extraction application for extracting a malicious code signature from said malicious code comprising:

locating a caller's address of said malicious code in a memory of said first computer system; and

extracting a specific number of bytes backwards from said caller's address;

said host signature extraction application further for creating an extracted malicious code packet including said malicious code signature; and

said host signature extraction application further for sending said extracted malicious code packet from said first computer system to a second computer system.

28. (Previously presented) A computer system comprising:

an intrusion prevention application for detecting an attack by malicious code on a first computer system;

a host signature extraction application for creating an extracted malicious code packet including parameters associated with said malicious code, said parameters being selected from the group consisting of a caller's address of said malicious code in a memory of said first computer system, a name of a process in which said attack took place, ports connected to said process, service pack levels, operating system information, patch level information, and combinations thereof; and

said host signature extraction application further for sending said extracted malicious code packet from said first computer system to a second computer system.

29. (Previously presented) A computer system comprising:

a local analysis center signature extraction application for receiving an extracted malicious code packet from a first computer system with a second computer system, said first computer system being a host computer system and said second computer system being a local analysis center computer system; and

said local analysis center signature extraction application further for determining whether an attack threshold has been exceeded based upon said extracted malicious code packet, wherein upon a determination that an attack threshold has been exceeded, said method further comprising delivering a signature update comprising a malicious code signature to an intrusion detection system.

30. (Previously presented) The method of Claim 1 wherein the specific number of bytes is 32 bytes.

31. (Previously presented) The method of Claim 9 wherein said malicious code is sendable if a size of said malicious code is 8 KB or less.

32. (Previously presented) The method of Claim 13 wherein said extracting a snippet comprises:

locating a caller's address of said malicious code; and extracting a specific number of bytes above and below said caller's address.

33. (Previously presented) The method of Claim 32 wherein said extracting a specific number of bytes above and below said caller's address comprises extracting 4 KB above said caller's address and 4 KB below said caller's address.

Evidence appendix

None

Related proceedings appendix

None

Conclusion

If there are any questions relating to the above, please telephone the undersigned Attorney for Applicant.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on November 30, 2007.

Attorney for Applicant(s)

November 30, 2007
Date of Signature

Respectfully submitted,

Serge J. Hodgson
Attorney for Applicant(s)
Reg. No. 40,017
Tel.: (831) 655-0880